IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: L. Garren Du et al.	Art Unit	: 3621
Serial No.	: 09/879,267	Examiner	: Jalatee Worjloh
Filed	: June 12, 2001	Conf. No.	: 3522
Title	: DIGITAL CONTENT PUBLICATION		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

(1) Real Party in Interest

The real party in interest is Accenture Global Services, GmbH, a corporation of Switzerland having a place of business at Neuhausen am Reinfall, Switzerland, as evidenced by an assignment executed between October 12, 2001 and October 17, 2001 and recorded at the U.S. Patent Office on February 12, 2002 at Reel 012613, Frame 0380.

(2) Related Appeals and Interferences

Neither Appellant, nor Appellant's legal representative, nor the assignee are aware of any appeals or interferences that will directly affect or be affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

No claims are allowed. Claims 1-40, 43, 44, and 50-55 are pending and on appeal. Of these, claims 1, 14, 27, 40, and 54 are independent.

(4) Status of Amendments

All amendments have been entered.

(5) Summary of Claimed Subject Matter

In an effort to avoid repetition of large amounts of text, Applicant provides the following table of passages that will be referred to in connection with the summary of claimed subject matter:

Passage	Location in Text	Text
A	page 13, line 9 to page 13, line 14	The DCP system 18 can include memory 52, such as, for example, read only memory (ROM), random access memory (RAM), static random access memory (SRAM), dynamic random access memory (DRAM), or other memory which can be connected to the CPU 56 through system bus 53. The CPU 56 can execute programs running in memory 53 and process data residing in memory 53.
B	page 8, line 13 to page 8, line 16	The DCP system 18 communicates with a digital content management (DCM) system 12 to retrieve unprotected digital content 16 and metadata 14 associated with the unprotected digital content.
C	page 18, line 21 to page 19, line 2	Protecting can include storing the digital content 22 in the DCP system 18 instead of sending the content to another system such as the DRM system or the content distributor 28. As a result, the DCP system 18 maintains control over the digital content.
D	page 9, line 16 to page 9, line 19	The DCP system 18 can produce protected digital content 22 by extracting the unprotected digital content 16 from the DCM system 12 and encrypting and storing the protected content into the DCP system 18.
E	page 17, line 21 to page 17, line 24	Once the DCP module 68 begins executing in the DCP system 18, the module can receive 104 the metadata associated with the unprotected digital content 16 that had been previously selected by the content publisher.
F	page 9, line 19 to page 9, line 22	The DCP system 18 can provide the content publisher 32 with a program module 68 to allow publication information 20 related to the protected digital content 22 to be entered.
G	page 19, line 13 to page 19, line 18	The message can be implemented using, for example, a set of application program interface (API) function calls that can establish a connection to the DRM system 24 using a password and user name. The message can be implemented using an XrML rights label containing metadata information and

		publication information associated with the digital content 22.
H	page 19, line 10 to page 20, line 4	The DCP system 18 sends 110 a message to the DRM system 24 over the network 26 indicating that the metadata and the publication information associated with the digital content 22 is available. The message can be implemented using, for example, a set of application program interface (API) function calls that can establish a connection to the DRM system 24 using a password and user name. The message can be implemented using an XrML rights label containing metadata information and publication information associated with the digital content 22. The XrML rights label may also contain the location of the digital content 22, an encryption protection key, and rights for using the protected content. The XrML also can register the content 22 with the DRM system 24; however, the content is stored in the DCP system 18 and not in the DRM system. The DRM system 24 can then extract the information from the label and store it in the label database. Once the label representing the content is registered with the DRM system 24, the content distributor 28 may access the label information to populate their Web-catalog.
I	page 12, line 8 to page 12, line 10	The DCP system 18 can include a central processing unit (CPU) 56 such as an Intel Pentium Processor.
J	page 13, line 22 to page 13, line 24	A DCP module 68 can be a program in memory 52 that can provide the functionality of digital content publication system according to the invention.
K	FIG. 3, step 104	
L	FIG. 3, step 110	
M	FIG. 3, step 106	
N	FIG. 3, step 108	
O	page 10, line 4 to page 10, line 12	The DRM system 24 is capable of processing extensible rights markup language (XrML) labels 23 generated by the DCP system 18. The XrML labels 23 can include the publication information and metadata data information

		associated with the digital content 22. XrML is an open specification for describing rights, fees, and conditions for using digital content over a network. The DRM system 24 can be a server computer connected to the network 26 and can include a label database 38 that can be used to store the XrML labels 23.
P	page 10, line 21 to page 11, line 4	The DRM system 24 also can include a license generator 32 which can be used to generate an encryption license permitting the protected digital contents 22 to be accessed by a content consumer 30. A license can be requested by the content consumer 30 through the content distributor 28. The license can be transferred to a content consumer 30 after the consumer has been validated or authorized to access the protected digital content 22.

1. A computer-implemented method comprising:	
receiving digital content (16) and metadata (14) associated with the digital content;	A, D, E, K
receiving publication information (20) comprising distribution information that identifies one or more content distributors (28) selected to distribute the digital content;	F, M
storing the digital content at a first computing system (18); and	C, G, N
sending the metadata (14) and the publication information (20) to a second computing system for storage separately from the first computing system (18).	H, L

14. A digital content publication apparatus comprising:	
a memory unit (52); and	A
a processor (56) configured to:	I
receive digital content (16) and metadata (14) associated with digital content,	B, D, E, K
receive publication information (20) comprising distribution information that identifies one or more content distributors (28) selected to distribute the digital content,	F, M

store the digital content at a first computing system (18); and	C, G, N
send the metadata (14) and the publication information (20) to a second computing system (24) for storage separately from the first computing system (18)	H, L

27. An article comprising a computer-readable medium that stores computer executable instructions for causing a computer system to:	J
receive digital content (16) and metadata (14) associated with the digital content;	B, D, E, K
receive publication information (20) comprising distribution information that identifies one or more content distributors (28) selected to distribute the digital content;	F, M
store the digital content at a first computing system (18); and	C, G, N
send the metadata (14) and the publication information (20) to a second computing system (24) for storage separately from the first computing system (18).	H, L

40. A system comprising:	
a digital content publication (DCP) computer (18) configured to receive digital content (16) and metadata (18) associated with the digital content from a digital content management (DCM) computer (12), receive publication information (2), store the digital content (22) at the DCP computer, and send the metadata and the publication information to a digital rights management computer (24) for storage separate from the DCP computer; and	B, D, E, K, F, M, C, G, N, H, L
a digital rights management (DRM) computer configured to receive the metadata and the publication information from the DCP computer, and store the metadata and the publication information, the publication information comprising distribution information that identifies one or more content distributors (28) selected to distribute the digital content.	G, O

54. A computer-implemented method for distribution of digital content, the method comprising:	
storing metadata (14) for digital conent (22) in association witih the publication information (20) for the digital content, the publication information identifying one or more content distributors (28) selected to distribute the digital content, the metadata being stored separately from the digital content, and	H, L, F, M
enabling secure distribution of the content according to the stored publication information.	P

(6) Grounds of Rejection to be Reviewed on Appeal

1. Independent claims 1, 14, 27, and 40 stand rejected as being rendered obvious under 35 USC 103(a) by the combination of Sasaki and Niwa.

(7) Argument

SASAKI

Sasaki[1] teaches a way to distribute encrypted digital content to content distributors **24** and to end-users **26**, **28**. This content is packaged into "transfer files." *Sasaki's* FIG. 4 shows the anatomy of a transfer file.

Referring to FIG. 4, the transfer file contains within it:

- an encrypted content package **147**; and
- certain information that one would need to decrypt the content package (i.e. the encrypted content key **148** and header information **133**).

The encrypted content package **147** contains a header **139** and the actual digital content **141**. A computing system receives both the header **139** and the content **141**. On the basis of

[1] *Sasaki* et al., US 2002/0077988.

information in the header **139**, the receiving computing system determines the extent to which it may play or distribute the content **141**.

NIWA

Niwa[2] teaches a system for enabling a user to view a sequence of video clips. These clips are automatically selected to conform to that user's particular interests. According to *Niwa*, prior art systems merely splice together video clips. As a result the viewer encounters discontinuities, which *Niwa* calls "jump cuts."[3] *Niwa* teaches a system for avoiding such jump cuts.

The video clips (video **132** in *Niwa*'s FIG. 1) and information about the video clips (description **132** in *Niwa*'s FIG. 1) are stored in a content database **36**. According to *Niwa*, although the video clips and information about the video clips are stored within the same content database **36**, they can be stored on separate storage media. Thus, *Niwa* contemplates the possibility that the descriptions **130** and the video clips **132** might, for example, be stored on different hard drives.

MAPPING SASAKI AND NIWA TO CLAIM 1

The Examiner regards *Sasaki's* header **139** as containing the "metadata" of claim 1 and the content **141** as being the "digital content" of claim 1. The header **139** includes a distributor ID **135**. The Examiner apparently regards this distributor ID **135** as being the "publication information" of claim 1. Accordingly, in the Examiner's view, any system that receives a transfer file inevitably carries out steps (1)-(3) of claim 1. That system would then become the "first computing system" of claim 1.

The Examiner concedes that *Sasaki* fails to teach step (4) of claim 1. Thus, the Examiner has correctly observed that whenever a computing systems in *Sasaki* receives a transfer file, that system inevitably stores *both* digital content *and* metadata.

To remedy *Sasaki*'s failure to teach step (4) of claim 1, the Examiner draws attention to *Niwa's* teaching of a content database **36** having a description file **130** and a video file **132** stored

---

[2] *Niwa*, US 2003/0225696.
[3] *Niwa*, paragraph 4.

on different storage media. In doing so, the Examiner apparently regards *Niwa*'s description file **130** as claim 1's "metadata" and *Niwa*'s video file **132** as being claim 1's "content." Since video file **132** and description file **130** can be on different storage media, the Examiner regards the placement of files in *Niwa* as evidence that the missing step (4) of claim 1, namely the step of

> "sending the metadata and the publication information to a second computing system for storage separately from the first computing system"

must have occurred.

Proposed modification would render Sasaki unsatisfactory for its intended purpose

Applicant draws attention to *In re Gordon*,[4] which stands for the proposition that if the proposed modification "would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification."[5]

The intended purpose of the *Sasaki* system is to prevent misappropriation of copyrighted content. *Sasaki* achieves this by providing each computing system with *both* the content *and* certain metadata that tells the computing system the extent to which that content can be played or distributed. If, as the Examiner suggests, the metadata and content were to be stored on different systems, it would follow that a computing system would lack either the metadata or the content. As a result, the *Sasaki* system would no longer be able to carry out its intended purpose.

To see this clearly, we consider how *Sasaki*'s system would function for each of the four possible modifications:

- The first possibility is that the user **26**, **28** (i.e. the media player) has the metadata but not the content. In that case, the user **26**, **28** would know it had permission to play content, but it would not have any content to play.

[4] *In re Gordon*, 733 F.2d 900 (Fed. Cir. 1984).
[5] *MPEP* 2143.01(V), referring to *In re Gordon*.

- The second possibility is that the user **26**, **28** (i.e. the media player) has the content but not the metadata. In that case, the media player would encounter no limit on the extent to which it can play or redistribute the content.

- The third possibility is that the commercial distributor **24** has the metadata but not the content. In that case, the commercial distributor **24** could provide a user **26**, **28** with permission to play content, but not the content itself.

- The fourth, and final, possibility is that the commercial distributor **24** has the content but not the metadata. In that case, the commercial distributor **24** could provide the user **26**, **28** with content, but would have no way of controlling either the playing of that content or its subsequent redistribution.

It is apparent that in the first and third of the four possible modifications along the lines proposed by the Examiner, the *Sasaki* system would fail to carry out its intended purpose, which is to prevent misappropriation of digital content. In the second and fourth of the possible modifications, the *Sasaki* system would be unable to even distribute content. Therefore, the proposed modification would render the prior art unsuitable for its intended purpose. Accordingly, and consistent with *In re Gordon*, the proposed modification cannot be a basis for a prima facie obviousness rejection.

Proposed modification changes Sasaki's principle of operation

Applicant draws attention to *In re Ratti*[6] for the proposition that if the proposed modification would change the principle of operation of the prior art invention being modified, then the teachings of the references are insufficient to render the claims obvious.[7]

Sasaki relies heavily on the presence of both the header **139** and content **141** in the same computing system. The presence of both components enables the computing system to determine the extent to which it may play the content. Separating the header **139** and content **141** as proposed would change this fundamental principle of operation of the *Sasaki* system.

[6] *In re Ratti*, 270 F.2d 810 (CCPA 1959).
[7] *MPEP* 2143.02(VI).

For example, if a media player had only the content **141** but not the header **139**, it would be unable to determine, by itself, the extent to which it can play particular content. This means the media player would have to retrieve the metadata from some remote database over a network each time it sought to play certain content. As a result, the media player could no longer be used in places in which it lacks continuous access to some sort of network, e.g. in an airplane, or in a remote location.

The proposed modification would thus change the principle of operation of the *Sasaki* system. In particular, the proposed modification would mean that a media player would have to consult a remote database every time it was asked to play content.

This modification not only changes the principle of operation but also the end result. For example, under the Examiner's proposed modification, the media player could no longer operate independently of a network.

Hence, the proposed motivation to combine the references leads to a drastic change in the principle by which the *Sasaki* system operates. This change in the principle of operation leads to a significantly different result. Accordingly, under *In re Ratti*, the proposed modification cannot be a basis for an obviousness rejection.

No motivation to combine the references

The rejection is a hindsight reconstruction, using applicant's claim as a template to reconstruct the invention by picking and choosing isolated disclosures from the prior art. This is impermissible under the law. For example, in *In re Fritch*, 972 F.2d 1260, 1266, 23 USPQ2d 1780, 1784 (Fed. Cir. 1992), the Federal Circuit stated:

> It is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious. *In re Gorman*, 933 F.2d 982, 987, 18 USPQ2d 1885, 1888 (Fed. Cir. 1991). This court has previously stated that "[o]ne cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." (quoting *In re Fine*, 837 F.2d at 1075, 5 USPQ2d at 1600)

The present rejection fits the court's description of what may not be done under § 103. The examiner has merely listed certain components of applicant's invention and then located isolated disclosures of those components. The law requires more than that.

The examiner must show where the prior art provides a motivation to combine the references he/she has combined in the obviousness rejection. Absent a motivation to combine, obviousness has not been demonstrated. As the Federal Circuit stated in *Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 934, 15 USPQ2d 1321, 1323 (Fed. Cir. 1990):

> It is insufficient that the prior art disclosed the components of the patented device, either separately or used in other combinations; there must be some teaching, suggestion, or incentive to make the combination made by the inventor.

"The initial burden is on the Examiner to provide some suggestion of the desirability of doing what the inventor has done."[8] "To support the conclusion that the claimed invention is directed to obvious subject matter, either

> the references must expressly or impliedly suggests the claimed invention or
>
> the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references."[9]

It is quite evident that the first prong of the above test has not been met. The references themselves fail to suggest the claimed invention. To see this, we examine the references in turn:

We begin with *Sasaki,* which teaches the idea of packaging the content with the metadata together into one "transfer file." This integration of content and metadata in a stable transfer file is a central aspect of *Sasaki*'s teaching. The Examiner's suggestion that one of ordinary skill in the art would have found it obvious to separate metadata from content is thus completely at odds with *Sasaki*'s statement that

---

[8] *MPEP* 2142.
[9] *Ex parte Clapp*, 227 USPQ 972, 973 (BPAI 1985).

> "***each*** digital work transmission involves the packaging of the digital work ***and*** the associated content header into an encrypted transfer filed that may be securely transmitted from one participating entity into another"[10]

One of ordinary skill in the art, having read and understood *Sasaki*, would promptly recognize that without the metadata, the media player would have no way of knowing what license restrictions would exist. This would make it easier to misappropriate copyrighted material, which is precisely the opposite of *Sasaki's* intended purpose. One of ordinary skill in the art would have no doubt recognized this obvious difficulty and would therefore have had no reason to separate content from metadata.

We turn next to *Niwa*, which teaches that when providing a sequences of video clips, one can store the video clips and information about the clips on separate storage media, which may or may not be on different computing systems. *Niwa* does not explain why either configuration offers offer any advantage over the other. Thus, one of ordinary skill in the art who reads *Niwa* would have no reason to ascribe any particular importance to where exactly one stores video clips and information about the clips.

It is therefore clear that *Niwa* offers no suggestion to one of ordinary skill in the art about whether to store content and metadata together on the same computing system, or separately, on different systems.

Since neither *Niwa* nor *Sasaki* can be said to expressly or impliedly suggest the claimed invention, the first prong of *Clapp* is not met. We therefore turn to the second prong, namely whether or not the examiner has presented "a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references."

The Examiner offers two different lines of reasoning for why one of ordinary skill in the art would have found it obvious to modify *Sasaki* to store content separately from metadata. The first reason is that doing so

---

[10] *Sasaki*, paragraph 40, [emphasis supplied].

> "helps to reduce unauthorized usage of content. That is, such a storage arrangement prevents the users from editing an expired filed to extend their usage term."[11]

The second reason is that doing so

> "promotes quick data transmission by reducing the amount of information stored on a data storage device"[12]

We first consider the first of the Examiner's two reasons: namely reducing the risk of unauthorized tampering.

According to *Sasaki*, the computing system associated with the end user is a portable media device, such as an MP3 device.[13] The Examiner appears to be suggesting that the owner of such a device, which lacks any significant programming interface to begin with, could, at least in principle, somehow tamper with an encrypted content package in such a way as to favorably modify his license.

However, *Sasaki* says nothing about the possibility that a determined programmer with sufficient skill could carry out what the Examiner suggests. In fact, *Sasaki* states that one advantage of his method is that "potential new customers are exposed to the digital content being offered…*without* substantial risk of unrestricted distribution of the digital content."[14] Thus, the Examiner's speculation on the possibility that one could tamper with the metadata could not have arisen from *Sasaki*.

Niwa has nothing to do with misappropriation of digital content. Instead, *Niwa* is directed to smoothly splicing video clips to avoid jump cuts. There is no suggestion in *Niwa* to store content **141** and metadata **139** on different computers in an effort to discourage a user from

---

[11] *Office Action*, page 6.
[12] *Id.*
[13] *Sasaki*, paragraph 35 ("users **26**, **27** may access and distribute digital content using a portable media device **80** which is configured to store, render and distribute digital content in accordance with instructions embedded in metadata associated with each digital work stored in the device") and paragraph 37 ("the portable media player may be implemented as a solid state MP3 player, a CD player, an MCD player, a camera, a game pad, a cellular telephone, or other electronic device").
[14] *Sasaki*, paragraph 39.

tampering with metadata **139**. This is because in *Niwa*, the metadata **139** does not play a role in restricting access. Its function is to describe the video clips. A user who chose to tamper with the metadata **139** in *Niwa* would thus gain no advantage, and would most likely cause incorrect video clips to be shown. Therefore, the Examiner's idea that a user would tamper with the metadata in an effort to overcome access restrictions could not possibly have arisen from *Niwa* either.

It is quite apparent therefore that there would be no reason to modify *Sasaki* to reducing the likelihood of tampering.

We now consider the second of the Examiner's two reasons, namely that one of ordinary skill in the art would modify *Sasaki* to achieve more rapid data transmission.

The Examiner appears to be suggesting that the *Sasaki* system could transmit data more rapidly from one computing system to another if only one were willing to give up transmitting the header together with the content.

While this is undoubtedly true, it would also mean that the recipient computing system could do anything it wished with the content. After all, the restrictions on what the recipient could do with the content would be kept in the header, which the Examiner, in his enthusiasm to reduce the amount of data sent, would have chosen to leave behind.

One of ordinary skill in the art would recognize that the purpose of the *Sasaki* system is to prevent misappropriation of copyrighted material. Therefore, if one of ordinary skill in the art sought to increase transmission speed in *Sasaki*, he would no doubt find a solution other than leaving metadata behind. One solution might be, for example, to transmit a lower resolution copy of the content, or to improve data compression methods. Certainly, one of ordinary skill in the art would never dream of withholding the very header information that makes the *Sasaki* system work.

Moreover, it is unclear how *Niwa*'s separation of description **130** and video **132** into different storage media can be viewed as having anything to do with transmission speed. As best

understood, the *News* metadata **130** is used in connection with selecting video clips at the server. There is no need to transmit the metadata **130** to the user.

Independent claims 14 and 27 recite limitations similar to those recited in claim 1, and are therefore patentable for at least the same reasons. All claims dependent on claims 1, 14, and 27 are patentable for at least the same reasons as their respective parent claims.

Claims 54 and 55 likewise recite "metadata being stored separately from the digital content." These claims are patentable for at least the same reasons as those discussed in connection with claim 1.

Summary

Enclosed is a petition for extension of time with authorization to charge our deposit account. Please charge the brief fee of $500 to our Deposit Account No. 06-1050, referencing Attorney Docket No. 12587-015001. No other fees are believed to be due in connection with the filing of this appeal brief. However, to the extent fees are due, or if a refund is forthcoming, please adjust our deposit account.

Respectfully submitted,

Date: May 23, 2007

Faustino A. Lichauco
Reg. No. 41,942

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

Appendix of Claims

1. A computer-implemented method comprising:

receiving digital content and metadata associated with the digital content;

receiving publication information comprising distribution information that identifies one or more content distributors selected to distribute the digital content;

storing the digital content at a first computing system; and

sending the metadata and the publication information to a second computing system for storage separately from the first computing system.

2. The method of claim **1** wherein receiving digital content includes receiving digital content from a digital content management (DCM) system.

3. The method of claim **1** wherein receiving publication information includes receiving publication information using a graphical user interface (GUI).

4. The method of claim **1** wherein the digital content includes at least one of streaming video content, music content, graphic content, print content, sound content, or audio content.

5. The method of claim **1** wherein metadata includes at least one of a name, length, publisher, location, or description associated with the digital content.

6. The method of claim **1** wherein publication information further comprises at least one of pricing, rights, or catalog information associated with the digital content.

7. The method of claim **50** wherein producing protected digital content includes encrypting the digital content and storing the encrypted digital content into a file transfer protocol (FTP) directory such that the digital content is accessible over a network.

8. The method of claim **50** wherein producing protected digital content includes encrypting the digital content and storing the encrypted digital content into a real server transfer protocol (RSTP) directory such that the digital content is capable of being streamed over a network.

9. The method of claim **50** further comprising producing thumbnail information associated with the digital content and storing the thumbnail information into a hypertext transfer protocol (HTTP) directory such that the thumbnail information is accessible over a network.

10. The method of claim **50** wherein producing protected digital content includes controlling access to the digital content over a network.

11. The method of claim **10** wherein controlling access includes using an XrML (eXtensible Rights Markup Language) license.

12. The method of claim **1** wherein sending includes sending a rights-label to a digital content rights management system (DRM), wherein the rights-label includes metadata and publication information associated with the digital content.

13. The method of claim **1** further comprising notifying a digital content distributor of the availability of the metadata and publication information associated with the digital content, the content distributor being one of the identified content distributors.

14. A digital content publication apparatus comprising:

a memory unit; and

a processor configured to:

receive digital content and metadata associated with digital content,

receive publication information comprising distribution information that identifies one or more content distributors selected to distribute the digital content,

store the digital content at a first computing system; and

send the metadata and the publication information to a second computing system for storage separately from the first computing system.

15. The apparatus of claim **14** wherein the processor is configured to receive digital content from a digital content management (DCM) system.

16. The apparatus of claim **14** wherein the processor is configured to receive publication information using a graphical user interface (GUI).

17. The apparatus of claim **14** wherein the digital content includes at least one of streaming video content, music content, graphic content, print content, sound content, or audio content.

18. The apparatus of claim **14** wherein metadata includes at least one of a name, length, publisher, location, or description associated with the digital content.

19. The apparatus of claim **14** wherein publication information further comprises at least one of pricing, rights, or catalog information associated with the digital content.

20. The apparatus of claim **14** wherein the processor is configured to encrypt the digital content and store the encrypted digital content into a file transfer protocol (FTP) directory such that the digital content is accessible over a network.

21. The apparatus of claim **14** wherein the processor is configured to encrypt the digital content and store the encrypted digital content into a real server transfer protocol (RSTP) directory such that the digital content is capable of being streamed over a network.

22. The apparatus of claim **14** wherein the processor is configured to produce thumbnail information associated with the digital content and store the thumbnail information into a hypertext transfer protocol (HTTP) directory such that the thumbnail information is accessible over a network.

23. The apparatus of claim **14** wherein the processor is configured to control access to the digital content over a network.

24. The apparatus of claim **23** wherein the control access includes using an XrML (eXtensible Rights Markup Language) license.

25. The apparatus of claim **14** wherein the processor is configured to send includes sending a rights-label to a digital content rights management (DRM) system, wherein the rights-label includes metadata and publication information associated with the digital content.

26. The apparatus of claim **14** wherein the processor is further configured to notify a digital content distributor of the availability of the metadata and publication information associated with the digital content, the digital content distributor being one of the identified content distributors.

27. An article comprising a computer-readable medium that stores computer executable instructions for causing a computer system to:

receive digital content and metadata associated with the digital content;

receive publication information comprising distribution information that identifies one or more content distributors selected to distribute the digital content;

store the digital content at a first computing system; and

send the metadata and the publication information to a second computing system for storage separately from the first computing system.

28. The article of claim **53** further comprising instructions for causing the computer to produce protected digital content wherein the digital content is received from a digital content management (DCM) system.

29. The article of claim **27** further comprising instructions for causing the computer to receive publication information using a graphical user interface (GUI).

30. The article of claim **53** comprising instructions for causing the computer to produce protected digital content, wherein the digital content includes at least one of streaming video content, music content, graphic content, print content, sound content, or audio content.

31. The article of claim **53** comprising instructions for causing the computer to protect the digital content, wherein the metadata includes at least one of a name, length, publisher, location, or description associated with the digital content.

32. The article of claim **53** comprising instructions for causing the computer to produce protected digital content, wherein the publication information includes at least one of pricing, rights, or catalog information associated with the digital content.

33. The article of claim **53** comprising instructions for causing the computer to produce protected digital content including instructions to encrypt the digital content and store the encrypted digital content into a file transfer protocol (FTP) directory such that the digital content is accessible over a network.

34. The article of claim **53** comprising instructions for causing the computer to produce protected digital content including instructions to encrypt the digital content and store the encrypted digital content into a real server transfer protocol (RSTP) directory such that the digital content is capable of being streamed over a network.

35. The article of claim **53** comprising instructions for causing the computer to produce protected digital content including instructions to produce thumbnail information

associated with the digital content and to store the thumbnail information into a hypertext transfer protocol (HTTP) directory such that the thumbnail information is accessible over a network.

36. The article of claim **53** comprising instructions for causing the computer to produce protected digital content including instructions to control access to the digital content over a network.

37. The article of claim 36 comprising instructions for causing the computer to control access includes instructions for controlling access using an XrML (eXtensible Rights Markup Language) license.

38. The article of claim **27** further comprising instructions for causing the computer to send a rights-label to a digital content rights management (DRM) system, wherein the rights-label includes metadata and publication information associated with the digital content.

39. The article of claim **27** further comprising instructions for causing the computer to notify a digital content distributor of the availability of the metadata and publication information associated with the digital content, the digital content distributor being one of the identified content distributors.

40. A system comprising:

a digital content publication (DCP) computer configured to receive digital content and metadata associated with the digital content from a digital content management (DCM) computer, receive publication information, store the digital content at the DCP computer, and send the metadata and the publication information to a digital right management computer for storage separate from the DCP computer; and

a digital rights management (DRM) computer configured to receive the metadata and the publication information from the DCP computer, and store the metadata and the publication information, the publication information comprising distribution information that identifies one or more content distributors selected to distribute the digital content.

43. The system of claim **40**, wherein the metadata includes at least one of a name, length, publisher, location, or description associated with the digital content.

44. The system of claim **40**, wherein the publication information further comprises at least one of pricing, rights, or catalog information associated with the digital content.

50. The method of claim **1** further comprising protecting the received digital content to generate protected digital content.

51. The apparatus of claim **14** wherein the received digital content is protected to generate protected digital content.

52. The apparatus of claim **51** wherein the protected digital content is stored.

53. The article of claim **27** comprising instructions for causing the computer to produce protected digital content.

54. **A computer-implemented method for distribution of digital content, the method comprising:**

storing metadata for digital content in association with publication information for the digital content, the publication information identifying one or more content distributors selected to distribute the digital content, the metadata being stored separately from the digital content; and

enabling secure distribution of the content according to the stored publication information.

55. The method of claim **54**, wherein enabling secure distribution comprises:

generating a protected version of the digital content;

using the metadata and the publication information to control access to the protected version of digital_content.

Evidence Appendix

None

Related Proceedings Appendix

None